U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: InterAgency FireNET
Bureau/Office: Office of Wildland Fire
Date: October 1, 2018
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

Wildland fire management is an ongoing concern to the American public, and to the U.S. Department of the Interior (DOI) and the U.S. Department of Agriculture (USDA). Cooperation and coordination among agencies is critical to the success of wildland fire management and safety. The DOI Office of Wildland Fire (OWF) and Office of Chief Information Officer

(OCIO) are partnering with the USDA Forest Service (FS) to interconnect computing services for improved Fire Community communication, collaboration, and operations. This partnership supports the goals of the Service First initiative to provide seamless services and improve operational efficiency between DOI and USDA to attain a common national mission of protecting resources against wildland fires.

As the lead agency, the DOI is in charge of the procurement and management of the information technology applications (apps) that will be used by both agencies. The InterAgency FireNET (FireNET) is a cloud-based interagency email and collaboration information system, a collaborative environment created within the Google G Suite Enterprise environment. FireNET is a major external application provided by Google as a Software as a Service (SaaS) collaboration environment and is shared and used by both the DOI as the managing partner and the USDA to achieve the interagency national mission through enhanced collaborative and cooperative effort. FireNET supports the interagency dispatch and wildland fire camp operations across multiple Federal, state, and local agencies by providing fire personnel with a collaborative system that is equipped with an easily accessible secure network and mobile application capabilities.

FireNET includes the Fire Management Board Portal and Wildland Fire Information and Technology Portal where the users can research information related to the wildlife fire communities, and the FireNET Platform where the users can apply to register accounts or login to their account.

FireNET is implemented in the Google G Suite Enterprise environment via the FedRAMP-certified Google cloud service. Google G Suite Enterprise provides the required collaborative space including Gmail, Calendar/Contacts, Google Apps (Docs, Sheets, Forms, Slides), Google Drive (shared documents), Google Chat, Google+, and Google Sites (a structured wiki- and Web page-creation tool offered by Google as part of the G Suite productivity suite). The goal of Google Sites is for users to be able to create a team-oriented site where multiple people can collaborate and share files in a device agnostic and highly available environment. While the data included in the FireNET environment is focused primarily on responding to fire incidents, some personally identifiable information (PII) may be included in notification rosters, communications, administrative records, and fire operations community personal contact records, such as name, phone number, email address, and organization that are collected to support fire operations and fire incident response. FireNET creates collaboration workspace access to agencies' home business and shared business applications for DOI/USDA and non-Federal employees, and enables the interagency fire community to continuously and rapidly expand its collaborative base across the Federal, state, tribal and local government with enhanced collaborative technical capacity and information security management capability.

C. What is the legal authority?

U.S. Department of the Interior and Related Agencies Appropriation Acts; Protection Act of 1922 (16 U.S.C. § 594); Reciprocal Fire Protection Act of May 27, 1955 (69 Stat. 66; 42 U.S.C.

§ 1856a); Federal Land Policy Management Act of 1976 (43 U.S.C. § 1702); National Park Service Organic Act of August 1916 (16 U.S.C. § 1); National Wildlife Refuge Administration Act of June 27, 1998 (16 U.S.C. § 668dd); Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (42 U.S.C 5121 et seq); National Indian Forest Resources Management Act of 1990 (25 U.S.C. § 3101); Cooperative Forestry Assistance Act of 1978 (P.L. 95-313, 92 Stat. 365 as amended; 16 U.S.C. § 2101 (note), 2101-2103, 2103a, 2103b, 2104-2105); Service First Initiative (P.L. 106-291, § 330, 43 U.S.C. 1701, Stat. 996, as amended) and subject to reauthorization; 36 CFR - Parks, Forests, and Public Property; 16 U.S.C § 551 - Protection of National Forests, Rules and Regulations; 44 U.S.C. 22 - Presidential Records; Federal Information Technology Acquisition Reform Act, Title VIII Subtitle D of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291); Service First Public Law 106-291, October 11, 2000, Section 330, 43 U.S.C. 1701 Page 76; Service First Public Law 109-54, August 2, 2006, Section 428, Pages 48-57; Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130, Managing Information as a Strategic Resource; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011; Presidential Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12); Policy for a Common Identification Standard for Federal Employees and Contractors (OMB Memorandum M-11-11), February 3, 2011; 43 U.S.C. 1451 the Department of the Interior, Establishment; 44 U.S.C. § 3101, Records management by agency heads; general duties; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII Code: 10-000001914; FireNET SSP 2017

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

DOI training records are maintained under the DOI-16, DOI Learn, system of records notice, 70 FR 58230 (October 5, 2005) and 73 FR 8342 (February 13, 2008). Network user records are maintained under DOI-47, HSPD-12: Logical Security Files, 72 FR 11040 (March 12, 2007). DOI SORNs may be viewed on the DOI Privacy Program page at https://www.doi.gov/privacy/doi-notices.

The USDA/FS is an interagency user of the FireNET email and collaboration information system to communicate and collaborate on wildland fire management and safety. Records in this system may also be covered by system of records notices published by the USDA. The USDA/FS-52, Resource Ordering and Status System (ROSS - National Interagency Resource Ordering and Status System), 70 FR 2601 (January 14, 2005), may be used by agencies that are members of the interagency National Wildfire Coordinating Group (NWCG) and its cooperators, and contains records on individuals who participate in wildland fire protection and other incident activities including Federal, state and municipal employees, and private individuals (https://www.gpo.gov/fdsys/pkg/FR-2005-01-14/html/05-800.htm).

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address

☒ Employment Information
☒ Other: *Specify the PII collected.*

Interagency fire community users include executive leadership, fire chiefs, dispatchers, fire firefighters, support personnel, personal aircraft services, National Interagency Fire Center (NIFC) staff, and other accepted fire community responders. The users will voluntarily provide the following information on the FireNET Account Access Request Form:

- First, Middle, Last Name
- Business Email Address
- Current Phone Number
- Agency and Bureau/Office
- Normal Duty Location (City, State)
- ESN/IMEI/MEID Number (for Mobile device access)

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☒ State agency
☒ Other: *Describe*

FireNET was chartered under the Wildland Fire Information and Technology (WFIT) Board on December 12, 2015 and has been implemented through a phased in approach.

The Fire Communities might utilize "volunteers" in some cases to support fire response scenarios. The potential exists that volunteers could be granted limited access to FireNET for scheduling and resource reporting.

The PII of personnel of other Federal agencies, tribal agencies and local agencies will be collected at other implementation phases. The Interagency Fire communities can be expanded to include other Federal agencies, state, tribal, and local personnel based on incident needs. In the event that these external partners are included in the FireNET environment, applicable background investigation and vetting will occur in accordance with the FireNET account management process. Personnel that are vetted will be given access only to pertinent information within FireNET to support fire incident response, law enforcement activities, and emergency response. The system is operated in a cloud environment and can be accessed with authorized credentials from any internet connected device.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Website https://www.FireNET.gov
☒ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*

DOI authorized users will not be given separate accounts in FireNET. They can use their DOI issued account credentials to log into BisonConnect and utilize file sharing from within FireNET. This would allow BisonConnect to pass user account information to FireNET.

☐ Other: *Describe*

D. What is the intended use of the PII collected?

PII collected includes work-related information such as the official email addresses of the users, which may include the user's First Initial and Last Name or First Name and Last Name and phone number. This information is used to identify the individual to the system and allow authentication, and for other system account management and security control purposes, and allows the Fire Community to communicate, collaborate, and manage operations.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

DOI Fire Community Bureaus will have access to contact information within FireNET. The specific bureaus and offices are Office of the Secretary, Bureau of Reclamation, U.S. Fish and Wildlife Service, U.S. Geological Survey, National Park Service, Bureau of Indian Affairs, Bureau of Land Management, and OWF. Information stored and processed within FireNET will be used to collaborate on activities associated with a fire incident.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

In the event of a fire incident which requires additional support, other DOI Bureaus and Offices not named above may be included in the sharing of data and communications in order to respond to the incident. Information stored and processed within FireNET will be used to collaborate on activities associated with a fire incident.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

USDA/FS personnel will have access to contact information provided within the FireNET system. Information stored and processed within FireNET will be used to collaborate on activities associated with a fire incident.

USDA/FS is the administrative agency for the ROSS system, which may be used by agencies that are members of the interagency NWCG and its cooperators. Information in the ROSS system may be disclosed to and used by the members of NWCG to perform their duties which might be part of the collaboration activities conducted via FireNET.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

In the event of a fire incident which requires additional support, Tribal, state and/or local agencies could be included in the sharing of data and communications in order to respond to the incident. Information stored and processed within FireNET will be used to collaborate on activities associated with a fire incident.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors were involved with the design and development of the system and its maintenance and operation.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals consent when they voluntarily provide information when requesting access to FireNET and can choose to decline. The FireNET Account Access Request Form contains a Privacy Act statement that informs users of the purpose and uses of their information and the voluntary nature of the form.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

A Privacy Act Statement is provided in the FireNET Account Access Request Form.

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is also provided through the publication of this privacy impact assessment and the published DOI-47 and USDA system of records notices.

☒ Other: *Describe each applicable format.*

DOI and USDA have their own internal procedures and forms that cover requirements and management of providing account information for access into FireNET. These processes and forms may include agency specific notice on the policies and requirements for acceptable use, expectation of privacy, and use of information collected for issuance and use of government-issued equipment, however, the privacy controls and security controls of FireNET are consistent which provide required protections for all the users. In addition, all DOI employees are notified via DOI Departmental policy, mandatory security awareness training, DOI Rules of Behavior and the DOI/USDA Warning Banner for use of FireNET that employee use of government-issued equipment and the FireNET network is subject to monitoring and information provided from individuals may be monitored to ensure the authorized use and security of FireNET information.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data can be retrieved from the system in various ways. This depends upon the privilege level of the user (e.g., administrator (privileged account) or user (non-privileged account) or system (built in capability such as auditing)). The data retrieval methodology is also dependent upon the application (e.g., Gmail, Drive, Calendar, etc.) that the user is currently using to retrieve data. FireNET Gmail emails specific to the user account can be retrieved by From-and-To username, From-and-To e-mail address, email subject, attachment name, size and date. The vault, drive, and sites can be searched by email sender and email recipient, subject, message ID, keywords, and date. Each FireNET G Suite application (e.g., Gmail, Drive, Calendar, etc.) has unique filters that can be used to search for information within the application. More information about this capability can be obtained within the Google Help file drop down. Generally, each application that makes up the G Suite offering has individually tailored search capability. Users are limited in their ability to search for information. System administrators can search and audit on more fields within G Suite.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

As a course of operating the FireNET system, reports will not be generated based on individuals. However, reports can be produced for troubleshooting and incident response purposes that include information on individuals. In these cases, the information is used to identify issues with the system or in response to an unauthorized or malicious activity. This capability is required for FireNET to be compliant with Federal and DOI IT security controls. Additionally, reports will be produced to properly manage user accounts.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

The users are required to complete the FireNET Account Access Request Form before being granted access right to the system. The users provide their full name and username. They may edit and update their own contact information within the FireNET system. The accuracy is verified by the user's manager and by the FireNET system administrator who creates the account. Dormant or inactive accounts are disabled after 60 days of non-use. The user is notified of the dormant account and asked to log in to prove continued need for an account. If the user does not comply within a reasonable time period, the account is deleted.

B. How will data be checked for completeness?

The users provide their names (first, last) and username. Individuals will have the ability to edit their own contact information from within the FireNET system. If the FireNET Account Access Request Form is not fully completed, no data is entered into FireNET nor is an account created until all required information is provided.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

USDA/FS and DOI fire personnel provide their names (first, last) and username. Individuals have the ability to edit their own contact information from within the FireNET system. The accuracy is verified by the user's manager and by the FireNET system administrator who creates the account. Dormant or inactive accounts are disabled after 60 days of non-use. The user is notified of the dormant account and asked to log in to prove continued need for an account. If the user does not comply within a reasonable time period the account is deleted.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Retention periods for FireNET data vary as records in FireNET are maintained by subject matter in accordance with the applicable bureau or office records schedule, or General Records Schedule, approved by the National Archives and Records Administration (NARA) for each specific type of record maintained by the Departments.

The System Maintenance & Use files for the system-related data of DOI are covered by the Departmental Records Schedule (DRS) 1.4.0013 record retention schedule. The disposition is temporary, cut off when superseded or obsolete, and destroyed no later than 3 years after cut-off.

The fire management records currently fall under the interagency records schedule previously negotiated between the pertinent DOI bureaus and the FS that apply to records created by interagency fire incident management teams under disposition authority N1-095-05-2, Item 3. The disposition is temporary, cut off at end of calendar year in which incident is termination. The records will be transferred to offsite storage three years after cutoff, and destroyed seven years after cutoff. This disposition authority for DOI records, will be superseded by DRS 2.1.5.0018 (DAA-0048-2015-0001-0018), pending approval. USDA/FS records will continue to fall under the N1-095-05-2, Item 3.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Records are disposed of in accordance with the applicable records retention schedules for each bureau or office, Departmental policy and NARA guidelines. Paper records are shredded and records contained on electronic media are degaussed or erased in accordance with 384 Department Manual 1.

Per service contractual requirements, the vendor will coordinate with DOI to ensure the identification, storage, retrieval, preservation, access and disposition of records solely using the DOI's Email Enterprise Records and Document Management System (eERDMS).

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

FireNET is a cloud-based enterprise-level application and a collaborative interagency system of DOI and USDA/FS. The data collected and stored in the FireNET environment will include some personal contact information, such as name, personal cell phone number, personal email address, and the work phone number and work email address of the fire operation community users composed of the employees and volunteers of DOI, USDA, State, Local and Tribal agencies, and other organizations, and members of the public as part of the fire community. PII will be used to support interagency dispatch and wildland fire operations and fire incident

response. There are privacy risks and potential impacts throughout the information management life cycles. To mitigate the privacy risk, a series of administrative, physical and technical controls have been implemented.

There is a risk that individuals may not have notice or be able to consent to the collection of information, the purposes for collection or how the information will be used. FireNET has set up a collection and consent process. A Privacy Act Statement is provided in the FireNET Account Access Request Form which is used solely for authorizing the fire operation community users to access the system and perform their job duties. This privacy impact assessment and the related published system of record notices inform the system users of the routine uses of the PII, the category of the PII and other required information legally maintained in the system. This collection and consent process ensures that no PII is collected and maintained in FireNET without the users' acknowledgement and consent.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. These privacy risks are mitigated through the following measures: FireNET is designated as a FISMA moderate system pursuant to the criteria outlined in Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems", and is hosted by a FISMA/FedRAMP-certified cloud services vendor. More than three hundred specified controls are mandated to be implemented by the service provider and the system owner, including strict access controls. All communications within the FireNET system are encrypted. The data stored within the system is also encrypted via proprietary Google algorithms. FireNET has also incorporated a Data Loss Prevention (DLP) tool and special security tool which can identify, block, and alert on sensitive PII data that is included in email or requested for sharing, which further enhances the system's technical capability to mitigate the privacy risk. DOI has signed an interagency agreement with USDA and will do so with all the other fire communities that recognize and maintain the information security program to ensure the implementation of security measures are readily secured, consistently achieved and effectively monitored, therefore, well-protect the PII.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. FireNET is hosted by a FedRAMP certified service provider and has met all requirements for information categorized as Moderate in accordance with FISMA. The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the moderate level. The use of FireNET is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and NIST guidelines. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information, and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

There is a risk that information may be used outside the scope of the purpose for which it was collected. The personnel, including the fire community users of both USDA/FS and DOI, are

required to complete security and privacy training prior to being granted an account within the FireNET system, and annual refresher training thereafter. The training specific to the uses of FireNET will also be provided to the users to ensure the system is used in accordance with its security configuration and unique mission needs. All the users of DOI systems are required to take annual privacy training and role-based training, which further enhance the privacy and security awareness of the users and strengthen the overall privacy risk management aptitude of the organizations.

There is a risk that the system may collect, store or share more information than necessary, or the information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored is limited to the minimal amount of data needed to support the fire community and meet Federal records requirements. Records are temporary and are maintained and disposed of after three years in accordance with records retention schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The minimum required information collected and maintained is necessary for creating and managing user accounts and for system management purposes.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable since the system does not derive new data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users

Users will have access to generic organizational access by default. All user created data are restricted to the owner. Sharing of data must be explicitly approved by the owner of the data before being able to view, edit or collaborate on information.

☒ Contractors

Contractor staff will be used to augment DOI and USDA/FS fire personnel. They will have access to generic organizational data by default. All user created data is restricted to the owner. Sharing of data must be explicitly approved by the owner of the data before being able to view, edit or collaborate on information. Contractor accounts will be deactivated when no longer required.

☒ Developers

DOI Federal and contract staff may be used to develop or implement further functionality within FireNET. These individuals will be granted access to the environmental configuration and not direct access to user data.

☒ System Administrator

System Administrators are DOI Federal staff that have access to configure the system, review audit logs, delegate access, create accounts, and respond to issues identified by the users.

☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

User access is determined based on need-to-know and least privilege principles. For organization users, the account access right is only granted through a formal account request process. The data owners determine their data access delegation. The setting for user data access is private by default. Any change to the default setting requires new granting process. Only authorized system administrators can access the system. The access to audit logs will be granted to system administrators on a limited basis.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Yes, contractors were involved with the design and development of the system and will be involved with the maintenance and operation of the system. Federal Acquisition Regulation (FAR) contract Clause 52.224-1, Privacy Act Notification (April 1984), FAR contract Clause 52.224-2, Privacy Act (April 1984), FAR contract Clause 52.239-1, Privacy or Security Safeguards (Aug 1996) and 5 U.S.C. 552a are included by reference in the agreement with the contractor. The contractual provisions also include the Foundation Cloud Hosting Services (FCHS) Information Technology Privacy and Security Requirements that DOI service providers must comply with.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The system will generate and maintain audit logs of user actions as mandated by DOI and Federal IT security policy. The information will be used by IT security and forensics professionals when investigating security incidents. The audit logs may also be used by a system administrator to help troubleshoot and fix user reported problems. User location can be estimated based on the originating IP address which, however, is not specific to the user's location, only the general location of the source would be logged.

Audit of user activity such as login, logoff, failed login, changes to sharing permissions, and email (time, sender, recipient, sender IP, Recipient IP and MessageID) are captured as part of the auditing of the system. Targeted monitoring of users activity within the system may be performed if requested, this will only be done with the request and approval of DOI and/or bureau/office IT staff, human resources, and responsible supervisor, and the parameter of the audit log will remain the same.

DOI has a contract with BetterCloud to use its application to improve the FireNET security posture or monitoring. BetterCloud provides audit log monitoring and alerting capabilities, enhanced DLP features, compliance rulesets, and file sharing audit capabilities. BetterCloud improves DOI's ability to automate security incident alerting and reporting on compliance and unauthorized activities conducted within the FireNET environment.

The tool must also provide the facility to monitor and audit an individual account. This tool, once configured for an account, must be able to track and record (journal) each time a message is received by or sent to the monitored account. The tool should be able to monitor chat and draft messages if necessary. The tool is capable of monitoring more than one user at a time. The monitoring tool must also provide a method to easily filter a specific user's messages or conversations.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

Throughout the troubleshooting or incident response processes information such as username, Name (First, Last), document ownership, and file permissions could be collected from the individual account. Time/date of file actions, email delegations or permissions changes made by the user can be viewed. Audit of user activity such as login, logoff, failed login, changes to sharing permissions, and email (time, sender, recipient, sender IP, Recipient IP and MessageID) are captured as part of the auditing of the system.

M. What controls will be used to prevent unauthorized monitoring?

Access to audit logs will be granted to system administrators on a limited basis, and only authorized system administrators who have been given a username and password will be able to access the system. The principle of least privileges will be applied. In addition, all users must complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter. All FireNET administrative staff must also complete role-based privacy and security training.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☒ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior

☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

FireNET System is a Service (SAAS) provided by Google and has been evaluated against the requirements established by FedRAMP and is continuously monitored by the vendor as well as DOI security personnel for potential lapses in security.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

DOI as the lead agency in the procurement and management of the information technology applications used by both DOI and USDA Forest Service. The Director of the Office of Wildland Fire serves as the FireNET Information System Owner and the official responsible for oversight and management of the FireNET security and privacy controls and the protection of information processed and stored by the FireNET system. The Information System Owner and the Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in FireNET. These officials are responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, as well as meeting the requirements of the Privacy Act in coordination with Privacy Act system managers, including adequate notice, making decisions on Privacy Act requests for notification, access, amendments, and complaints in consultation with DOI Privacy Officials.

DOI has signed interagency agreement with USDA to jointly recognize and accept each other's federal credentials and required federal security, privacy, and records management training. All other users must complete the required federal security, privacy, and records management training offered through the DOI Learning Management System to be eligible to receive accounts and credentials for FireNET. This will ensure that users are aware of and trained to federal standards for information security, privacy information recognition and protection and records disposition and protection.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The FireNET Information System Owner is responsible for oversight and management of the FireNET security and privacy controls and for ensuring to the greatest possible extent that FireNET data is properly managed and that all system access has been granted in a secure and auditable manner. The Information System Owner is responsible for ensuring that any loss,

compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures.

DOI has signed interagency agreement with USDA and will do so with all the other fire communities pertaining to recognizing and maintaining the information security program that ensure the implementation of security measures can be readily secured, consistently achieved and effectively monitored, therefore well-protect the PII. The parties to the interagency agreement will be responsible for properly protecting all information used, gathered, or developed as a result of work under this agreement and for reporting any incidents involving PII.